Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 18 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- NBC4−TV reports that police warned Thursday, June 17, that a man has been stealing the ATM cards of people in eleven Orange and Los Angeles county, CA, cities, after tricking the victims into revealing their PIN numbers so he can get to their money later. (See item 8)
- The Associated Press reports that a part−time nurse at Chesapeake General Hospital, in Virginia, died of tuberculosis last week, prompting health officials to notify hundreds of people who may have come in contact with her. (See item 19)
- Reuters reports that some U.S. subscribers dialing 911 for emergency services on their mobile phones could find that their call is interrupted several times due to a recently discovered glitch in a new technology meant to pinpoint the caller's location. (See item 26)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 17, Associated Press* — **Atmos Energy acquiring more assets. Atmos Energy Corp. said Thursday, June 16, it is purchasing TXU Gas Co. in an all−cash deal worth $1.9 billion. Officials at Dallas, TX−based Atmos said the acquisition creates a gas utility with 3.1 million customers in twelve states.** TXU Gas is a wholly owned subsidiary of Dallas,TX−based TXU Corp. The deal, expected to close in the first quarter of Atmos Energy's 2005 fiscal year, is dependent upon limited regulatory approvals and other clearance. It was

unanimously approved by Atmos Energy's board of directors and does not require the approval of Atmos Energy shareholders. Last month, TXU Gas won approval from the Texas Railroad Commission to raise its rates, but not as high as the company wanted. TXU officials said residential customers will see their bills go up by an average of $2 a month.
Source: http://www.nytimes.com/aponline/business/AP−Atmos−TXU−Gas.ht ml

2. *June 17, Knight Ridder* — **World energy supply: Saudi oil targeted, experts say. Escalating sabotage against pipelines in Iraq is heightening fears that terrorists are planning a wholesale assault on energy targets throughout the region and are taking aim at the world's largest oil supplier −− Saudi Arabia.** The head of Saudi Arabia's government oil monopoly remains confident that the industry is well protected. However, independent experts warn that an attack on any of Saudi Arabia's major facilities could cripple world oil supplies. Experts warn that the country's pipelines, oil wells, refineries and export terminals are enticing targets for al Qaeda, whose operatives in Saudi Arabia are threatening to launch a devastating attack. Extensive terrorist attacks on oil targets in Saudi Arabia and Iraq would be tantamount to "an energy Pearl Harbor," forcing severe shortages and boosting prices in the United States and other countries heavily dependent on imported oil, said Anne Korin, a senior analyst with the International Institute for Analysis of Global Security in Rockville, MD. **The United States gets more than 50 percent of its oil from foreign suppliers. The terrorists "can hit the homeland without ever leaving their own backyard," Korin said.**
Source: http://www.freep.com/news/nw/saudi17_20040617.htm

3. *June 17, Federal Computer Week* — **Brody to lead Department of Energy cybersecurity. Bruce Brody, the cybersecurity chief at the Department of Veterans Affairs (VA), is moving to the Department of Energy to help that agency toughen its security against viruses and hacker attacks.** Brody is expected to start his new job as associate chief information officer for cybersecurity in mid−July. He is widely credited with helping the VA move from having a poorly secured cyber environment to having one of the best security plans in government, according to Robert McFarland, the VA's CIO. Pedro Cadenas Jr. will become VA's acting cyber− and information security chief, according to McFarland. In an interview, Brody said that the VA was once plagued with viruses. But after three years on the job, "it now has the largest and most effective antivirus implementation in government," he said. Brody, who has spent most of his career at the Department of Defense, said he will become the only cybersecurity chief to have experiences in two Cabinet−level departments. **He said he is looking forward to his new job because of its national security challenges. The Department of Energy has significant classified systems because it oversees nuclear facilities nationwide.**
Source: http://fcw.com/fcw/articles/2004/0614/web−brody−06−17−04.asp

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *June 17, United Press Interntional* — **Bacteria−fused chips make super sensors. By applying bacteria to microchips, NASA−backed researchers have created devices that can sense any number of chemicals, paving the way to future uses in space travel, homeland security, medicine, and environmental cleanup.** The devices −− called bioluminescent

bioreporter integrated circuits, or BBICs −− offer a low−cost, low−energy way to monitor their surroundings continuously to detect targeted substances. The attached bacteria act as exquisitely sensitive detectors, much as canaries once did when coal miners carried them underground to warn of the presence of odorless−but−deadly gases. Microbiologist Gary Sayler and colleagues at Oak Ridge National Laboratory in Tennessee tackled the problem by developing genetically engineered bacteria that glow blue−green in the presence of contaminants. They then joined the microbes to micro−luminometers −− chips designed to measure the minuscule amounts of light these germs emit. **The researchers combed genetic databases for microbes already known to detect a variety of compounds, such as solvents like ammonia or benzene; metals like copper, lead or mercury, and organic molecules like proteins or PCBs.**
Source: http://www.upi.com/view.cfm?StoryID=20040616−014617−7716r

[Return to top]

Defense Industrial Base Sector

5. *June 17, Government Computer News* — **House committee passes $416 billion DoD bill. The House Appropriations Committee on Wednesday, June 16, approved a $416 billion fiscal 2005 Defense spending bill that gives "measured adjustments" to programs that support military transformation** In the spending plan proposal, legislators also set aside $25 billion in emergency defense spending to pay for operations in Iraq and Afghanistan. **The proposal provides "increases in support of military transformation while making measured adjustments to ensure that future costs, as well as development, testing and production profiles, are efficiently managed," according to a release on the plan.** Other highlights include $2.9 billion for the Army's Future Combat Systems, a project to develop networked combat vehicles and weapons systems, and 2) $4.4 billion to the Navy and Air Force for development of the F−35 Joint Strike Fighter, a high−tech combat aircraft program that received $4.3 billion this year. The Senate is considering its version of the fiscal 2005 spending bill.
Source: http://www.gcn.com/vol1_no1/daily−updates/26247−1.html

[Return to top]

Banking and Finance Sector

6. *June 17, Associated Press* — **Online banking is clicking with more customers.** Millions of Americans are doing their banking online, and their ranks are expected to grow rapidly in coming years as more e−services become available and Internet connections get faster. **A study by comScore Networks released on Thursday, June 16, of online banking at the nation's ten largest financial institutions found that 22 million consumers logged in to their accounts in March, a nearly 30 percent increase from a year earlier.** Most went online to view their checking or savings account balances, the study showed. However, **many were monitoring their credit cards, paying bills, managing credit lines or paying mortgages.** Online banking use expanded more than tenfold from 1996 to 2003, TowerGroup Research, based in Needham, MA, said in a report last month. TowerGroup expects nearly 37 percent of

all U.S. households to be registered to bank online by 2007 −− a total of 42.5 million households. ComScore's study found that online bill paying has grown rapidly, but that there still is room for expansion. The results found that most consumers −− 84 percent −− still prefer to pay bills through a utility or merchant's site rather than through a bank site.
Source: http://seattletimes.nwsource.com/html/businesstechnology/2001957930_onlinebanking17.html

7. *June 17, CongressDaily* — **House chair calls for single anti−money laundering agency. Arguing that the nation's "fragmented" anti−money laundering system is structurally incapable of keeping pace with the war on terrorism, House Financial Services Oversight and Investigations Subcommittee Chairwoman Sue Kelly said Wednesday, June 16, that lawmakers should establish a single federal office to ensure compliance with the Bank Secrecy Act (BSA).** Dennis Schindel, Department of Treasury's acting inspector general, said audits have revealed gaps in various regulators' monitoring of financial institutions' BSA compliance efforts. "While it is evident from our work that Treasury takes its responsibilities very seriously, in almost every area we have audited we have identified problems significant enough to impact Treasury's ability to effectively carry out its role in combating terrorist financing and money laundering," Schindel said. A recent report, for example, found that the Office of the Treasury Secretary was "not aggressive" in taking enforcement actions against thrifts found to be in "substantial noncompliance" with BSA requirements, according to Schindel. Schindel said other audits have shown that Treasury's Financial Crimes Enforcement Network's database of suspicious activity reports has lacked critical information and contained inaccurate data.
Source: http://www.govexec.com/dailyfed/0604/061704cdam2.htm

8. *June 17, NBC4−TV (CA)* — **Police warn of ATM scam in southern California. Police warned Thursday, June 17, that a man has been stealing the ATM cards of people in eleven Orange and Los Angeles county, CA, cities, after tricking the victims into revealing their PIN numbers so he can get to their money later. The suspect places plastic objects or adhesive tape inside the ATM card slot, which causes a person's card to be "captured" inside the machine,** said Irvine police Lt. Jeff Love. The suspect, who stands nearby and feigns talking on a cell phone, advises the customer to enter a personal identification number and press cancel to get the machine to release the card. The man then watches as the victim punches in a PIN, then walks away, Love said. When the card does not come out, the victim eventually leaves. Then the suspect returns, retrieves the card, takes it to another cash machine and −− using the purloined PIN −− withdraws money, Love said. The scam has been reported in Santa Fe Springs, Fullerton, Alhambra, La Habra, Costa Mesa, Huntington Beach, Temple City, Covina, Garden Grove, Baldwin Park and West Covina, Love said.
Source: http://www.nbc4.tv/news/3429598/detail.html

[Return to top]

Transportation Sector

9. *June 17, USA TODAY* — **Airports to test bomb−sensing devices.** The Transportation Security Administration (TSA) is to unveil on Thursday, June 17, the first new bomb−detection device in airports since the September 11 terrorist attacks −− machines that blow air at passengers and

"sniff" for explosives. The agency is testing the machines to find out whether they work well enough to install them at every airport in the U.S. Airports in Providence, RI, Tampa, FL, San Diego, CA, and Rochester, NY, will test the detectors for 45 days, TSA officials said. If the machines prove practical, they will help close a gap in security. **Travelers now pass through metal detectors, and their carry−on bags are X−rayed, but most people boarding a plane are not searched for explosives. Chemicals used to make bombs cling to clothes and skin for weeks, even after washing. The government is testing new machines designed to detect these chemicals on airline passengers, which could become a new weapon against terrorists.** TSA officials said the test will tell them whether the machines are reliable and can be used on large numbers of passengers without causing delays. The machines take up to 15 seconds per person, which is slower than metal detectors.
Source: http://www.usatoday.com/travel/news/2004−06−16−bomb−detect−u sat_x.htm

10. *June 17, Las Vegas Review−Journal* — **Monorail safety net in place. Las Vegas Monorail officials in Nevada are betting that security guards, surveillance cameras and other features will keep commuters safe after the rail line opens later this summer.** In late May, the U.S. Department of Homeland Security issued a directive ordering passenger rail operators to implement various protective measures. Todd Walker, a monorail spokesperson, said the monorail system's security will be evident without being too onerous to the more than 50,000 people expected to use the system each day. Guards will be posted at every monorail station and may be traveling on the driverless trains at times. Each station will have a dozen or more cameras, and each train car will be outfitted with a pair of cameras. Images will be fed back to the monorail's control room, where technicians will monitor operations around the clock. **Walker said passengers and bags will not be screened, but security staff will keep an eye out for suspicious or unattended packages.** Trash cans, which can be used to hide a bomb, have been removed from monorail stations.
Source: http://www.reviewjournal.com/lvrj_home/2004/Jun−17−Thu−2004/news/24119663.html

11. *June 17, CNN* — **Air defense chief: 9/11 planes could have been downed.** The head of U.S. military air defenses on Thursday, June 17, said his fighter jets could have shot down the four hijacked airplanes September 11 if communication had been better between the Air Force and civilian air controllers. During Thursday's hearing of the 9/11 commission, Air Force Gen. Ralph E. Eberhart was asked whether it would have been "physically possible" for U.S. fighters to intercept the planes, if everything had gone perfectly. Eberhart responded: "I assume in the preface to your question −− you assume that FAA told us as soon as they knew, and if that is the case, yes, we could shoot down the aircraft." **Eberhart, commander of the North American Aerospace Defense Command, said NORAD and the Federal Aviation Administration have improved response strategies since the attacks. If those changes had been in place on September 11, the air defenses would have been able to intercept all four planes, he said.**
Source: http://www.cnn.com/2004/ALLPOLITICS/06/17/911.commission/ind ex.html

12. *June 17, WTOL−TV− (OH)* — **Barge hits CSX rail bridge. Crews have now dislodged a tug and barge from the mouth of the Maumee River. The Coast Guard says the tug "Michigan" and a barge carrying 40,000 barrels of gasoline hit the CSX rail bridge just north and east of downtown Toledo, OH.** It happened just after 9:00am Thursday, June 17, as

the barge was fighting the currents in the Maumee River. Several tugs were able to free the barge just after 12:00 noon. No one was hurt, and no gasoline was spilled. CSX says about 13 trains are being held up, since the bridge is stuck in the open position. The CSX Operations Center says train crews are also being told to be aware of crossings, and try not to block them. CSX crews are already inspecting the bridge to see what damage has been done.
Source: http://www.wtol.com/Global/story.asp?S=1949476&nav=5UagNzna

[Return to top]

Postal and Shipping Sector

13. *June 17, DM News* — **Higher fuel costs hurting USPS.** Postmaster general John E. Potter warned that the drastic increase in fuel costs is harming the U.S. Postal Service (USPS). "With a fleet of more than 210,000 vehicles that cover a billion miles every year," Potter said, "high fuel prices hit us hard." USPS vehicles consume 800 million gallons of gasoline and diesel fuel annually. **"Since January, regular gasoline costs have climbed about 38 percent," Potter said. That increase produced spending of about $80 million above what the postal service had budgeted.** Potter also noted that high fuel prices have increased heating and electricity costs for the postal service's 38,000 facilities. Mailers last week said they are growing concerned about how rising gas prices will affect the next postage rate increase, which most likely will occur in 2006.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2869 3

[Return to top]

Agriculture Sector

14. *June 17, Detroit Free Press (MI)* — **Bass virus spreading. Largemouth bass virus was first found in Florida's Lake Weir in 1991. The disease has since spread to 17 states. After the virus was first seen, it took only nine years to show up in Lake George on the Michigan−Indiana border.** "What has us somewhat concerned is that we don't know how the virus works on the northern subspecies (of largemouth bass) or in northern waters," said Gary Whelan, the fisheries production manager for the Michigan Department of Natural Resources (DNR). The virus seems to kill adult bass, mostly fish bigger than two pounds, but Whelan said that could be because "we don't see the smaller ones that die." **Wherever there has been an outbreak, it has killed about 10 percent of the largemouth bass population.** "It first showed up in Lake George in 2000, and now we've confirmed it in 15 other lakes," Whelan said. The virus also has been found in smallmouth bass, bluegill and redbreast sunfish, and crappies, as well as guppies and some minnows, but it doesn't harm those related species. Whelan said: "We're not going to cure it, but we do want to try to manage around it. We're going to look at sunfish, minnows, even suckers to try to discover the vector by which the disease is transmitted."
Source: http://www.freep.com/sports/outdoors/bass17_20040617.htm

15. *June 16, Animal and Plant Health Inspection Service* — **Funds for animal identification system. The U.S. Department of Agriculture's (USDA) Animal and Plant Health**

Inspection Service (APHIS) Wednesday, June 16, announced that it is accepting funding applications from state and tribal governments to support the initial implementation of the national animal identification system (NAIS). A total of $11.64 million will be available for implementing an identification system for all livestock and poultry animals on farms and ranches. "A national animal identification program will better equip the government and industry with the means necessary to quickly control a variety of animal disease outbreaks and reduce the economic impacts on the market," said Ron DeHaven, APHIS administrator. In April, more than $18 million was transferred from USDA's Commodity Credit Corporation to APHIS to begin implementing a national system that will quickly trace diseased or potentially diseased animals to their point of origin. Of this amount, more than $11 million is available for state and tribal governments to focus chiefly on premises identification. The remainder of the funds will be used to support the development of the national animal identification program.
Source: http://www.aphis.usda.gov/lpa/news/2004/06/vs_animidgrant.ht ml

[Return to top]

Food Sector

16. *June 17, Food Navigator* — **EU says no to GM food crop.** Europe rejected the entry of a genetically modified (GM) food crop supplied by biotech giant Monsanto into the food chain with officials from the 25 member states failing to reach a qualified majority at the vote Wednesday, June 16. **The UK, Denmark, and Italy voted against allowing the GM oilseed rape, also known as GT73, onto the market** while France, The Netherlands, and Sweden chose the "for" camp. The vote came in at 43 for and 57 against, with 24 states abstaining. A total of 88 votes for is required for a qualified majority. **The major food use of rape, also known as canola, in North America and Europe is as a refined vegetable oil.** But with the 25 member states failing to reach a qualified majority yesterday on allowing Monsanto's oilseed rape, designed to resist the company's chemical herbicide, into the European Union, the decision is now shunted onto the council of ministers.
Source: http://www.foodnavigator.com/news/news−NG.asp?id=52912

17. *June 16, Food and Drug Administration* — **Almond recall. Royal Food International is conducting a voluntary recall on its distribution of raw whole almonds labeled as Almond Raw due to the possibility of contamination with Salmonella Enteritidis.** Salmonella is an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. In rare circumstances, infection with salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis. Royal Food International distributed these products to retail stores, cafes, and delis in New York, New Jersey, and Connecticut. This recall is in follow−up to a voluntary recall announced in mid−May by Paramount Farms of California of whole and diced raw almonds based on over 20 possible cases of illnesses associated with the almonds.
Source: http://www.fda.gov/oc/po/firmrecalls/rfi06_04.html

[Return to top]

Water Sector

18. *June 17, Associated Press* — **House panel approves funds for water pipelines. A project to pipe Missouri River water to people in three states is a step closer to receiving more federal funding, Rep. Stephanie Herseth, D−SD, said.** The House Appropriations Committee on Wednesday, June 16, approved more than $64 million for water development projects in South Dakota, including $17.5 million for the Lewis and Clark Rural Water project, which was left out of House funding last year. The funding also includes $18.2 million for Mni Wiconi water project and $17 million needed to finish construction on the Mid Dakota water system. Source: http://www.aberdeennews.com/mld/aberdeennews/news/8944606.ht m

[Return to top]

Public Health Sector

19. *June 17, Associated Press* — **Nurse dies from tuberculosis. A part−time nurse at Chesapeake General Hospital, in Virginia, died of tuberculosis, prompting health officials to notify hundreds of people who may have come in contact with her.** Chesapeake city health director Nancy Welch said patients and visitors who were on a medical−surgical unit on the second floor of the hospital between October and April will be receiving letters advising them to be tested for TB. Family members and friends of the nurse, and the staff at Chesapeake General Hospital, also are being tested. The nurse, who lived in Virginia Beach, died at Bon Secours De Paul Medical Center in Norfolk on Saturday, June 12. Norfolk and Virginia Beach health departments also are tracking anyone who had contact with her in those cities. Source: http://www.dailypress.com/news/local/virginia/dp−va−−tbdeath 0617jun17,0,2364129.story?coll=dp−headlines−virginia

20. *June 17, U.S. Department of Health and Human Services* — **HHS awards funds for public health preparedness. Health and Human Services (HHS) Secretary Tommy G. Thompson Wednesday, June 17, announced an additional $849 million in awards to states, territories, and four major metropolitan areas to strengthen the ability of government and public health agencies to respond to bioterror attacks, infectious diseases, and natural disasters.** This funding is in addition to $498 million released earlier this month by HHS Health Resources Services Agency to strengthen hospitals and improve overall response capability. All totaled since September 11, 2001, HHS has invested more than $3.7 billion in strengthening the nation's public health infrastructure. Recipients will be able to use the funds in a number of ways to improve public health and emergency response. These include improving communication and coordination between hospitals and local and state health departments, and their laboratories, while bolstering epidemiology and disease surveillance in state and local areas by increasing the number of people trained in emergency response. Source: http://www.hhs.gov/news/press/2004pres/20040617.html

21. *June 16, CIDRAP News* — **Study to probe cardiac effects of smallpox vaccine.** In an effort to shed some light on a potential side effect of smallpox vaccination, researchers are launching a federally funded pilot study of the effects of smallpox vaccines on cardiac cells in mice. **The general aim of the study is to begin investigating why smallpox vaccination appears to**

trigger myopericarditis (inflammation of the heart muscle and lining) in a tiny fraction of recipients, according to a news release from the North Carolina State University School of Veterinary Medicine. **Among more than 39,000 civilian health workers who received smallpox shots in 2003, there were 16 suspected and 5 probable cases of myopericarditis after vaccination,** according to the U.S. Centers for Disease Control and Prevention. **In addition, 75 cases of myopericarditis occurred among 623,244 military personnel who received smallpox shots between December 2002 and May 10, 2004,** according to the Department of Defense. North Carolina State officials said the National Institutes of Health awarded a two year, $500,000 grant for the research.
Source: http://www.cidrap.umn.edu/cidrap/content/bt/smallpox/news/ju n1604vaccine.html

22. *June 15, Associated Press* — **U.S. government says Canadian firms shipped unauthorized drugs south. Three Canadian pharmacies shipped unauthorized medication to Wisconsin residents, newly released documents alleged, underscoring U.S. government concerns about state and local programs that encourage cheap drug imports.** In separate letters dated April 27, the Wisconsin Department of Health and Family Services told Winnipeg−based CanadaDrugs.com, Granville Pharmacy of Vancouver, and Calgary's Total Care Pharmacy they had shipped generic drugs that were not approved for sale in the United States. CanadaDrugs.com also was criticized for improperly shipping an item needing refrigeration, insulin, to a Wisconsin resident. The U.S. Food and Drug Administration, which released the letters Tuesday, June 15, has vigorously opposed programs in Wisconsin and elsewhere to allow residents to import cheaper drugs from Canada, arguing they put Americans at risk for counterfeit and unsafe medications.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1843&ncid=18 43&e=4&u=/cpress/20040615/ca_pr_on_he/us_cda_drugs

[Return to top]

Government Sector

23. *June 17, Washington Post* — **Homeland Security to remain in Washington, DC. The Department of Homeland Security will keep its permanent headquarters in Washington, DC, for at least five years and possibly longer while it consolidates operations now spread across 5 million square feet of office space throughout the region,** Bush administration officials said Wednesday, June 16. Homeland Security, which has 180,000 workers across the country, plans to roughly double the number of top employees −− currently about 2,000 people −− who are based at the Nebraska Avenue Naval Complex, and spend $75 million on technological upgrades over five years. The Navy will move out 1,147 workers by January, said a spokesman for the Naval District of Washington. **This summer, the General Services Administration (GSA) expects to complete an inventory of all Washington area real estate occupied by the 22 agencies that are part of Homeland Security. The aim is to produce a "long−term housing strategy" for what is now the federal government's largest Cabinet department,** GSA capital area spokesman Mike McGill said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A47755−2004Jun 16.html

24. *June 17, National Oceanic and Atmospheric Administration* — **Homeland Security uses NOAA network for alerts. National Oceanic and Atmospheric Administration (NOAA)**

and the U.S. Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate Thursday, June 17, signed an agreement that allows Homeland Security to send critical all−hazards alerts and warnings directly through the NOAA All−Hazards Network. The Network supplements the existing alert and warning resources and the capability serves as an additional delivery mechanism for sending life−saving information nationally, regionally, or locally. In addition, Homeland Security's Federal Emergency Management Agency will continue to manage the Emergency Alert System that includes the NOAA All−Hazards Network. Under this agreement, Homeland Security now has the authority to develop an alert and warning message that can be delivered directly to NOAA and broadcast to affected areas. The system is capable of reaching over 97 percent of the U.S. territory on a 24 hour basis through broadcasts in 50 states, Puerto Rico, the Virgin Islands, Guam, and Saipan.
Source: http://www.noaanews.noaa.gov/stories2004/s2245.htm

[Return to top]

Emergency Services Sector

25. *June 17, LOCAL10.com (FL)* — **Terror drill tests local, state, federal readiness . Agencies from local, state, and federal levels in Florida joined together on Thursday, June 17, to test their responsive readiness in case of a terror attack.** The mock attack began at 6 a.m. in Monroe County in the Keys, moved into Miami−Dade and Broward counties throughout the morning and ended up at Port Everglades. The counties practiced working together to get the job done in a safe and effective manner. "If something is going to happen in multiple locations, it's going to put stress on law enforcement, on fire rescue, on health, on hospitals," said Broward County Sheriff Ken Jenne. One area agencies focused on was communication, which can often be difficult in a crisis, especially when so many agencies are trying to work together. **One lesson agencies learned is that they'll have to be quicker notifying the Department of Homeland Security when there is a terrorist threat.**
Source: http://www.local10.com/news/3429020/detail.html

26. *June 16, Reuters* — **Some Verizon Wireless 911 calls hit by GPS glitch. Some U.S. subscribers dialing 911 for emergency services on their mobile phones could find that their call is interrupted several times due to a recently discovered glitch in a new technology meant to pinpoint the caller's location, Verizon Wireless said** on Wednesday, June 16. The interruption is a side effect of technology Verizon uses to tell police and other emergency personnel a caller's location so that help can be dispatched as soon as possible, according to Verizon spokesperson Jeffrey Nelson, who said the company is fixing the problem. U.S. wireless operators have been working for years to meet regulatory requirements for giving location information to emergency services but progress has been slowed by new technology and the need to coordinate with thousands of safety organizations. Verizon Wireless uses a combination of network software and handset chips that hook up to Global Positioning System (GPS) satellites to pinpoint location. **The company has been able to set up the necessary network links to make the system work with only about 1,000 of the country's 6,700 local 911 call centers so far.**
Source: http://www.reuters.com/newsArticle.jhtml?type=technologyNews &storyID=5443047

27. *June 16, RAND Corporation* — **Study says new approach needed to protect emergency responders in terrorist attacks and disasters.** Better planning, training, coordination and management procedures are needed to protect emergency responders at the scene of terrorist attacks and disasters, according to a study issued on Wednesday, June 16, by the RAND Corporation and the National Institute for Occupational Safety and Health. The study proposes a new approach that would make protecting the health and safety of emergency responders a key priority in coordinating the overall response to terrorist attacks and major disasters. Currently, each agency that sends emergency responders to an incident takes responsibility for safeguarding its own workers. **Because terrorist attacks and major disasters often draw emergency responders from several departments in nearby communities −− with different operating procedures, communications systems and response plans −− coordinating efforts to protect workers is difficult, the report says. The study recommends enhanced preparedness planning to assure that all emergency responders to an event can be protected within the Incident Command System, the standard overarching management structure used in disaster response.** This would prevent different departments from wasting valuable time trying to come up with ways to protect workers on a case−by−case basis at each emergency scene. Study: http://www.rand.org/publications/MG/MG170/MG170.pdf
Source: http://www.rand.org/news/press.04/06.16.html

[Return to top]

Information Technology and Telecommunications Sector

28. *June 17, Associated Press* — **France Telecom, China Telecom partner.** France Telecom and China Telecommunications Corporation have signed a partnership pact and are opening a joint research and development center in China. In a statement Thursday, June 17, **the French group said it had concluded a "strategic partnership to launch a long−term collaboration in several areas of activity" with China Telecom, China's biggest fixed line operator.** China's official news agency, Xinhua, reported that the two companies had each agreed to invest $24 million in the first joint research center in Beijing.
Source: http://www.washingtonpost.com/wp−dyn/articles/A48691−2004Jun17.html?nav=headlines

29. *June 16, Govexec.com* — **Cybersecurity spending projected to be flat in 2005.** According to a report from consulting firm INPUT, government spending on IT security products and services is on track to increase by 2 percent from fiscal 2004 to fiscal 2005. By comparison, the same category increased 10 percent from 2003 to 2004, 50 percent from 2002 to 2003 and 100 percent from 2001 to 2002. The report comes after repeated warnings from Congress that the government's IT security is weak and poorly managed. Rep. Tom Davis, R−Va., chairman of the Government Reform Committee, also has kept pressure on federal agencies to increase IT security; he has warned of a "cyber Pearl Harbor" if defenses are not improved. **In its study, INPUT concluded that IT security shortfalls happen as agencies fail to follow cybersecurity guidance from the Office of Management and Budget (OMB).** Annual security reviews by OMB and Congress "have revealed a number of security lapses, unresolved from previous years, leaving many legacy systems vulnerable to attacks," said Chris Campbell, a senior analyst at Input. Campbell said the fiscal 2005 spending level will most likely be an aberration.

Source: http://www.govexec.com/dailyfed/0604/061604d2.htm

30. *June 16, InformationWeek* — **Bill would force federal agencies to toughen cybersecurity. Legislation to require federal agencies to account for cybersecurity when conducting information systems planning and acquisition was introduced Tuesday**, June 15, by two House leaders on federal government IT policy. **The bill, HR 4570, also grants the White House Office of Management and Budget greater authority to guide agencies on IT security issues.** Rep. Tom Davis, R.−Va., who chairs the House Government Reform Committee, pointed out that a high degree of interconnectivity exists between internal and external information systems, which exposes the federal government's computer networks to benign and malicious disruptions. In addition, he said, an agency's operational efficiency relies heavily on the productive use of technology. The bill, if enacted, would ensure that every federal IT system is managed in a way that minimizes the security risks.
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=22100133

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: Internet scans for backdoor and Trojan Horse ports continue to top the lists of all reporting organizations. The likely reason for such scans are that Bot Networks continue to amass zombie hosts from prior infected hosts such as Sasser and Bagel victims. The use of "botnets" to create denial of service attacks remain a serious threat to the National Infrastructure.

Current Port Attacks

Top 10 Target Ports	80 (www), 1026 (nterm), 1080 (socks), 9898 (dabber), 3128 (squid−http), 1025 (blackjack), 1434 (ms−sql−m), 5554 (sasser−ftp), 135 (epmap), 1027 (icq) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

31. *June 17, Agence France Presse* — **Special forces meeting to counter terrorism. Special forces and counter−terrorism officials from the U.S. and 14 Asia−Pacific nations were meeting in Australia this week in an unprecedented attempt to coordinate their war against al Qaeda and its Southeast Asian allies.** The three−day gathering, held in the rural town of Bowral south of Sydney, began on Wednesday, June 16. **"As unpalatable as it may**

be, we have to acknowledge that this region is a breeding ground for Islamic extremism," Australian Defense Minister Robert Hill told the meeting, which included special forces commanders and counter−terrorism officials from the U.S., China, Indonesia, Japan, Malaysia, the Philippines, Thailand, Singapore, and Vietnam. Other nations participating in the meeting, were Brunei, Cambodia, India, New Zealand, and Papua New Guinea. **Hill said that despite the arrest of key figures from al Qaeda and its main Southeast Asian ally, Jemaah Islamiyah, terror groups in the region remained "persistent, innovative, and adaptable".** "They continue to manage to execute relatively complex operations through meticulous operation planning and the engagement of previously unknown terrorist networks," he told the conference.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1512&ncid=721&e=12&u=/afp/20040617/wl_afp/australia_attacks_us

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.